THUNDER ADC MEETS MOBILE SERVICE PROVIDER NETWORK CHALLENGES

Safeguard and Optimize Service Availability with A10 Networks

Challenge:

Mobile service providers need to rapidly deploy innovative revenue-generating services. This demands intelligent and robust network infrastructure that scales to meet exponential traffic growth, optimizes the end user experience, ensures vital security and meets tight cost objectives.

Solution:

A10 platforms provide mobile service carriers a scalable, high-performance and comprehensive application delivery solution. These products support a broad array of critical functionality in a small, cost-effective appliance.

Benefits:

- Optimize network delivery of mobile communication traffic to value-added services
- Ensure continual service uptime through high availability, redundancy and robust hardware
- Heighten customer satisfaction with accelerated content delivery
- Consolidate numerous "point products" into one scalable ultra-high capacity appliance
- Defend both network infrastructure and applications against malicious multi-vector attacks

Mobile service provider challenges

The mainstream use of mobile communications has become ubiquitous, with enterprises of all sizes and consumers around the globe turning heavily to mobile for its universal coverage, expansive service offerings, inexpensive access and high-speed performance. Along with this increased user base has come exponential growth in data consumption, which is being driven by unlimited data rate plans, social media, over-the-top (OTT) applications and streaming video. In the United States alone, over three trillion megabytes of wireless data were sent in 2013[1]. This is nearly 50 times the traffic in 2008 and this figure is expected to increase eight-fold by 2018. The proliferation of advanced smartphones, tablets, connected homes and in the near future, automobiles, along with the need to support an increasing number of new mobile applications are magnifying the difficulties facing today's service providers.

Develop flexible networks that support advanced service offerings. Increasing competition and market pressure are driving the demand to innovate and quickly bring new and differentiated revenue-generating services to market. While service providers do not originate much of the content, they need to ensure delivery to the end user. To guarantee robust networks capable of providing current and future offerings, providers deploy specialized value-added service (VAS) platforms. This infrastructure handles mobile video optimization, ad insertion, unified communication, personalized content services and more.

Guarantee service delivery performance and availability. Mobile network operators must eliminate service disruption and ensure subscribers a positive customer experience. With the highly competitive mobile communications industry, even minor glitches in uptime will result in significant churn. Networks need to be architected for high availability and complete redundancy and use network elements with proven reliability. At the same time, the performance demands must be exceeded with highly scalable infrastructures and the ability to efficiently route traffic through the network to prevent bottlenecks and duplicative data processing. Network conversions from 3G/UMTS to 4G/LTM standards that have increased observed throughput by up to 100x have only exacerbated such demands.

Minimize infrastructure cost and rack space through use of consolidated platforms. Reduced wireline revenues from traditional telephony service and increased CAPEX/OPEX costs required to expand the mobile network infrastructure are twin burdens challenging financial results. Service providers have had to add substantial capacity to their radio access network as well as the packet core. Moving voice and multimedia communications to all packet-based technologies via IP Multimedia Subsystem (IMS) has added to the difficulties. Now the junction between the Gateway GPRS Support Node (GGSN) and the Internet with its SGi/Gi interface and the VAS portion of the network are drawing attention. To provide a cost-effective solution and overcome network operation center space constraints, providers must combine multiple disparate functions into as few components as possible.

[1]http://www.ctia.org/resource-library/press-releases/archive/ctia-annual-survey-2013

Ensure security of user sessions and the network elements. Mobile service providers need to protect their operations under the toughest conditions. Assaults that originate from the Internet, or other untrusted external networks that target the SGi/Gi interface of the mobile network infrastructure are particularly serious. Attackers can flood the mobile network with excessive requests and thus prevent legitimate subscribers from accessing the Internet. Inline stateful firewall and intrusion prevention system (IPS) solutions are innately vulnerable to Distributed Denial of Service (DDoS) floods that can overwhelm their capacity limits and, thus, are not sufficient protection.

A10 solutions for mobile service providers

With A10 Networks, mobile service providers can rapidly deploy new revenue-generating services, while guaranteeing the required network scalability, service availability and infrastructure security. Mobile communication networks can leverage the extensive feature set designed into A10 Thunder™ ADC product line of high-performance, next-generation application delivery controllers (ADCs), Carrier Grade Networking (CGN) and Threat Protection System (TPS) platforms.

Thunder ADC solutions ensure the necessary intelligent traffic management to offload high throughput data plane traffic to value-added services while handling complex control plane signaling in real time. With their comprehensive capabilities, Thunder ADC appliances replace multiple disparate point products to save cost, power and network operations rack space. CGN products provide the ability to extend limited IPv4 address space while supporting the migration to IPv6 and ensuring application reliability during address translations. With Thunder HVA hybrid virtual appliance platforms, up to 40 separate instances of both ADC and CGN can be installed on the same appliance.

A10 purpose-built designs include up to 150 Gbps of HTTP capacity, massive SSL processing support exceeding 40 Gbps, NEBS-compliant options, 1 rack unit designs, aVCS clustering for up to 8x scalability, and 100Gbps Ethernet ports to provide the power required by the most demanding of mobile environments.

Optimize traffic steering to value-added services

The pinnacle of the mobile operator's business model are value-added services that drive revenue and profitability. Such services enhance the customer experience and mitigate the impact of mobile traffic growth. These include:

- **Video optimization** – Condenses content size and bandwidth needs via transcoding and transrating. Augments the user experience for faster downloads and superior rendering.
- **Personalized content services** – This includes the ability to add parental control and URL filtering to block objectionable material. Targeted ad insertions can be realized along with reporting and fulfillment services. Filters are set and applied on a per-subscriber basis.
- **Wireless Application Protocol (WAP) gateway** – WAP manages the WML and HDML encode/decode process between the mobile device and the Internet. Multimedia apps, such as MMS, and JAVA downloads are enhanced.

In order to optimize these services, networks must go beyond traditional Layer 3/4 policy-based routers. Such legacy products route all traffic to every VAS platform and cause each device to inspect all traffic. This causes immense duplication of processing and the VAS infrastructure must be dramatically scaled up. With the rise of flat, all-IP networks such as with LTE, more application-level visibility with an intelligent subscriber network management system and policy enforcement is required.

Thunder ADC appliances with their full proxy and context-aware features enable centralized Layer 7 intelligent traffic management through traffic steering. This technique allows user requests to only be routed as needed, whether to VAS services, service provider content sources (i.e., web portal, commerce site) or OTT content from third parties, based on predetermined policies. User requests can be directed based on highly granular metrics such as data type, subscriber profile, server availability and requested service. For example, video
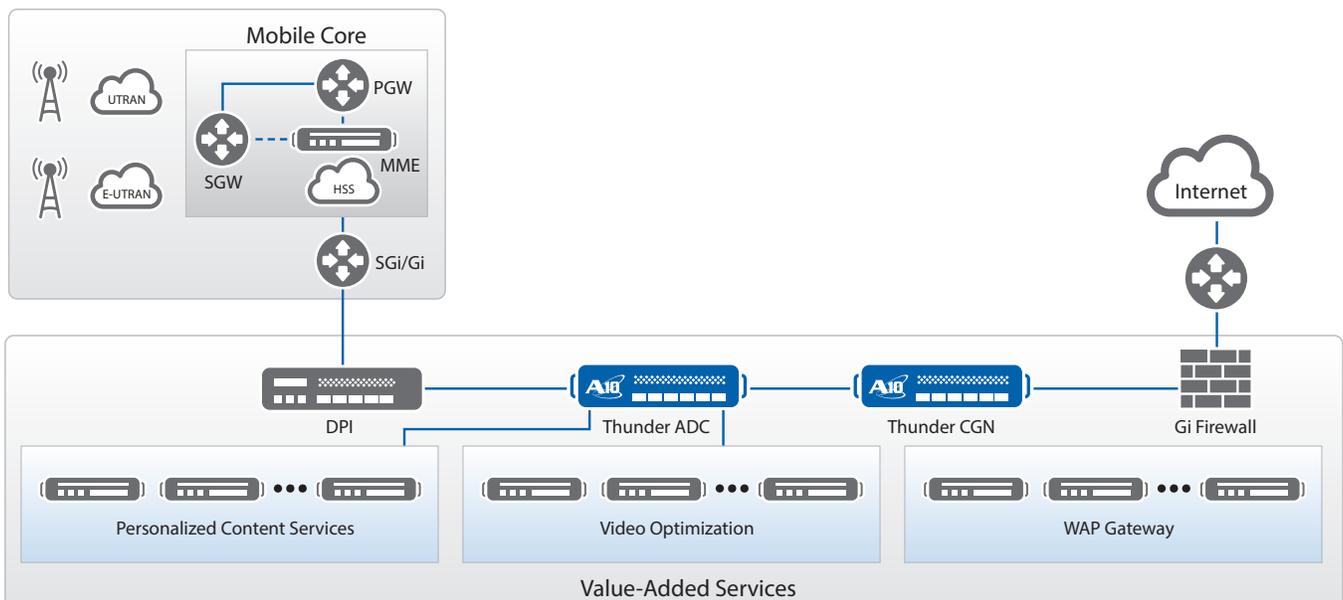
Figure 1: Mobile network with A10 Thunder ADC for intelligent traffic management to VAS services

traffic can be identified and only that content forwarded to the video optimization resource. This obviates the need to include cumbersome and costly traffic management features within each VAS platform. Thunder ADC-based traffic steering dramatically reduces scalability needs, redundant functionality and required VAS processing.

A10 can further improve network flows by the support for intelligent service chaining. Traffic can be identified by individual TCP connections and HTTP requests to allow the chaining of single sessions. Sessions entering the SGi/Gi interface are sequentially redirected across multiple VAS or other services for superior service levels, enhanced end user experience and optimized network efficiency. Persistence is maintained as required throughout the process. Service providers have the added flexibility of adding or updating the VAS platforms without affecting service availability or functionality; by load balancing traffic away from these impacted services, new revenue-generating services can be added with faster monetization.

Fortified service availability

With the expansion of new mobile offerings, real-time content management and the desire to provide tiered services, mobile service providers are turning to real-time policy engines. Deploying such capabilities involves adding or extending Policy and Charging Rules Function (PCRF), RADIUS and DIAMETER servers, Authentication, Authorization, and Accounting (AAA) and Subscriber Profile Repositories (SPRs). Combined with the increased use of data and voice transmission and high-speed LTE networks, the number of signaling connections per session in the control plane is dramatically escalating. This puts heavy burdens on the various servers, charging systems and IMS session management entities.

At the same time, with the exponential rise in user sessions and annual worldwide traffic flow now measured in Exabytes, the mobile infrastructure needs systems that can support this capacity. Every link in the data plane chain needs to keep up, including the traffic steering and service chaining segment. No network elements are 100 percent reliable, but the network as a whole must be. A key answer to ensuring network uptime is through deploying solutions that can detect failure and quickly switch over to redundant systems.

A10 Thunder ADC appliances provide solutions to maintain mobile network operation centers when failures occur. With their advanced load balancing, content switching and flexible health monitoring capabilities, service availability for network and server elements managed by Thunder ADC appliances is guaranteed. Intelligent traffic management is supported by numerous algorithms for maximum flexibility. Innovative health monitoring methods detect server downtime and failed services. Scriptable health checks detect response codes, response times, application errors and more to accurately pinpoint problems and route traffic to available servers.

Using the RADIUS protocol, Thunder ADC appliances manage and control traffic to application servers such as PCRF, AAA and SPR, and they support a variety of key protocols deployed at the SGi/Gi interface, including DNS, RADIUS, DIAMETER and NTP. A10 load balances and scales these servers to prevent overloaded control plane messaging. Data plane traffic to VAS services is also load balanced where traffic is steered to the various platforms based on availability to improve service reliability.

For additional availability support and expanded performance, A10 Networks aVCS™ Virtual Chassis System (aVCS) allows up to eight appliances to operate as a single device with centralized management. By clustering multiple devices, aVCS enables service providers to increase load balancing capacity, simplify management and lower cost. Service providers can deploy aVCS in conjunction with VRRP-a for redundant clusters. VRRP-a, like Virtual Router Redundancy Protocol (VRRP), eliminates single points of failure on the network, but VRRP-a also features sub-second failover and scalability of up to eight appliances in a failover group. Together, aVCS and VRRP provide horizontal scaling and stateful failover, meeting the high availability requirements of the largest mobile service providers.

Service and application acceleration

The TCP/IP protocols established decades ago were never expecting to see the worldwide mobile communications of today's environment. They were designed for high bandwidth and low latency networks, which are generally the opposite of current cellular systems. These rules for managing data transport are inherently inefficient and when coupled with network congestion result in packet loss, latency,
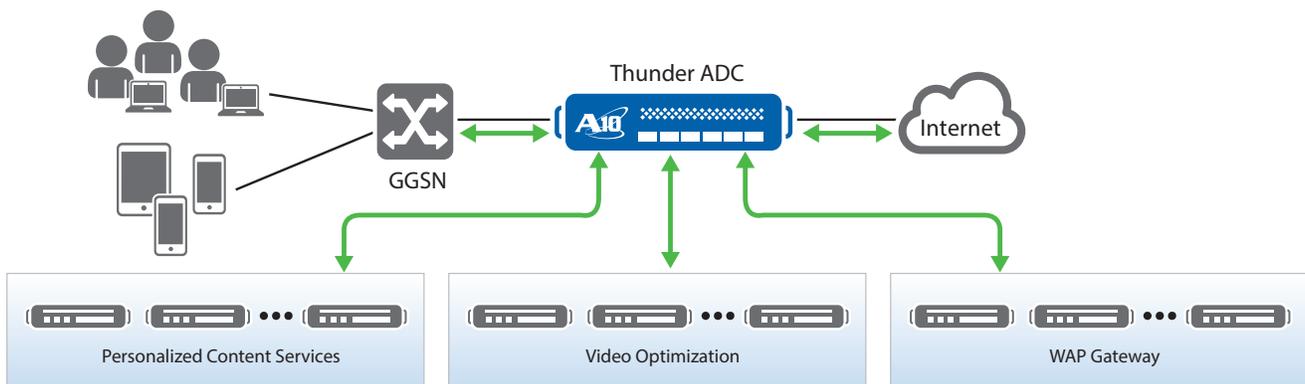
Figure 2. A10 Thunder ADC chains multiple services together

substandard application performance and bandwidth inefficiencies. To overcome these drawbacks, many standardized RFC extensions have been developed and adopted by network equipment vendors. By leveraging these TCP enhancements, application performance can be substantially improved in modern mobile service provider networks.

A10 solutions control and optimize the entire TCP-based communication process, including session initiation, three-way handshakes, window size, packet reordering and maximum transition unit size. This minimizes service congestion and latency. By overseeing TCP acknowledgements, error resolution and retransmission decisions, TCP sessions are more efficient for faster access and superior quality of service.

TCP optimizations are fully transparent with no modifications needed to the application servers or client devices. IT administrators are provided full control over the TCP stack to tune TCP communications as desired. Specific TCP variables that can be adjusted include: Delayed and selective acknowledgments, fast ramp, client keep-alive and window scaling. Such optimizations are fully compliant with network standards and are easy to configure. Resulting connectivity rates have been shown to double with much less bandwidth required.

A10 adds proprietary additions to further optimize TCP-based data transmissions. By using a full proxy architecture, A10 solutions separately negotiate mobile client-side and origin server-side connections. Each connection has its own windows scaling parameters to allow tailored connectivity for the mobile and LAN sides of the user session. Such a methodology obviates the need for client and server to negotiate the lowest common denominator when experiencing congestion. Each side of the connection is maximized to obtain the best achievable performance. The A10 appliance acts as an intermediary for the client to optimize the client-side delivery, while the same is done for the server side.

Simplify mobile communication architecture

With the proliferation of the network operations center to support advanced services while allowing the required capacity, mobile infrastructures have become incredibly complex. Going forward, securing scalability, supporting expanded services and reducing proliferating expenses will require operators to consolidate their topology. By utilizing advanced solutions, service providers can unite multiple point products, ease the operational management burdens and raise their ROI.

A10 provides all-encompassing products that merge numerous network elements into one easy to deploy appliance. These solutions unify intelligent traffic management, policy enforcement, security, address and protocol translations and SSL processing offload into a single platform. A10 Thunder designs institute a central control point for both data and control plane functions. The result is simplified network management with improved service performance as packet routing is minimized and TCP protocols are enhanced.

A10 Thunder appliances scale to meet the needs of the largest mobile service providers. Powered by A10's 64-bit Advanced Core Operating

System (ACOS®), these hardware platforms have the capacity to deliver up to 150 Gbps of intense Layer 7 processing in a one rack unit device. With aVCS clustering support, up to eight units can be grouped together with a "Super VIP" methodology for over 1 terabit/second of capacity. Each and every functional module may be utilized simultaneously to realize the needed network consolidation. With NEBS certification, solid state drives, redundant power supplies and 100 Gbps optical transceivers, these solutions have the necessary robustness and reliability for mission critical environments.

A10 Thunder designs also support virtualized deployments for added flexibility. For on-demand resource allocation of ADC and CGN functionality, vThunder™ offers an easy-to-deploy, full-featured virtual appliance. Mobile operators can provision added capacity with ultra-granular policy configurations on commodity servers with a wide range of hypervisor support. Thunder HVA hybrid virtual appliances combine the flexibility of vThunder virtual appliances with the performance of a hardware platform. Up to 40 fully isolated instances are supported on HVA models and both ADC and CGN instances can reside on the same appliance for increased consolidation.
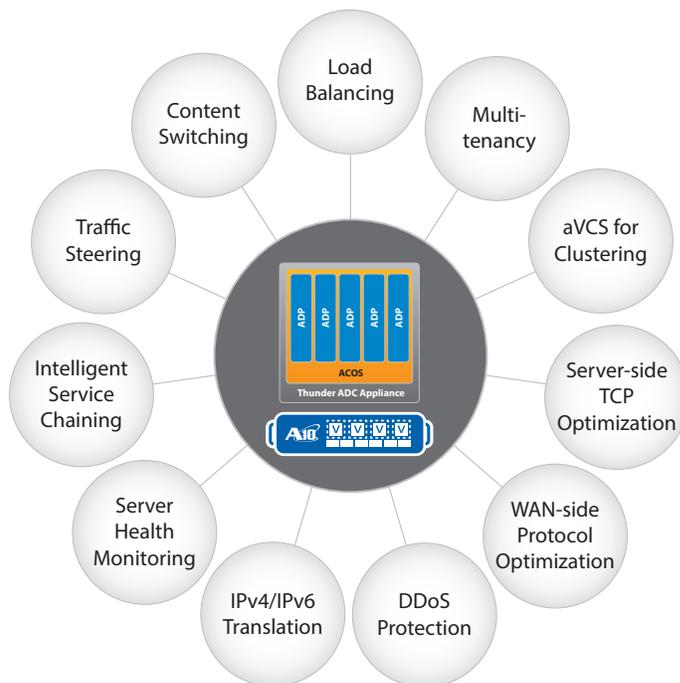
Figure 3. A10 Thunder ADCs consolidate multiple point product features into one space efficient appliance

Safeguard mobile services and network operations

With the advent of all IP-based mobile communication systems such as LTE, the once relatively closed "walled garden" ecosystem under the control of the service provider has ended. Unfortunately, this transformation has opened up more avenues to malicious intrusions. The SGi/Gi interface between the core network and external services, including the Internet, has particular security ramifications. Threats such as DDoS floods, application-layer attacks and DNS exploits

can arise from mobile phones infected with botnets as well as from anywhere within the Internet. Attacks may target the radio access network, VAS engines or the core itself threatening service availability. Network performance degrades and can become unavailable. Standard network firewalls are insufficient, as multiple attacks involving SYN, UDP and connection floods can overwhelm the firewall.

Thunder ADC purpose-built hardened appliances integrate extensive security features to protect the mobile service provider's infrastructure from a wide array of threats. Such a comprehensive solution allows the Thunder ADC installation to be at this vital Gi/SGi junction and handle not only inline traffic management and other capabilities, but simultaneously identify and eliminate incursions. The result is a highly efficient deployment where packet processing is minimized for superior quality of experience. A10 security for mobile communications includes:

- Layer 4 and Layer 7 DDoS and protocol anomaly protection, to prevent multi-vector volumetric attacks at up to 200 million SYN packets per second, including TCP, UDP and ICMP floods. Protects RADIUS, DNS, NTP and other control plane servers as well as the radio access network.
- ICSA-certified Web Application Firewall, to protect services and infrastructure under cyber attacks. Defends voicemail, email and messaging systems from potential vulnerabilities.
- DNS Application Firewall, to shield DNS servers from attacks including buffer overflow, malformed requests and DoS. IP-based connection rate limiting and concurrent connection controls mitigate DDoS assaults, including those arising from malicious DNS amplification.
- Enforcing DNS security extensions (DNSSEC), to verify DNS data. Ensures that DNS queries are from a trusted source to block DNS cache poisoning.
- Application Access Management (AAM), for web-based authentication.

Summary

A10 Thunder ADC platforms solve many of the challenges faced by today's mobile service providers. These powerful all-in-one solutions help operators realize the potential of their network infrastructure investments. They consolidate numerous "point products" into one scalable ultra-high capacity appliance while ensuring constant application and service availability. They defend both network infrastructure and applications against volumetric multi-vector attacks. They efficiently speed delivery on requested content to end clients. New services can be quickly brought to market and monetized with substantially reduced CAPEX and OPEX, all while simplifying deployment complexity and management. End users will benefit from superior mobile communication performance and enhanced network reliability, and this will help mobile service providers drive greater customer loyalty.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**